AMENDMENTS TO THE SPECIFICATION

Please delete the section entitled "SUMMARY OF THE INVENTION" in its entirety and substitute the following section therefor:

SUMMARY OF THE INVENTION

[0021] The present invention, among other applications, is directed to solving these and other problems and disadvantages of the prior art. The present invention provides a superior technique for performing cryptographic operations within a microprocessor. In one embodiment, an apparatus in a microprocessor is provided for accomplishing cryptographic operations. The apparatus includes a cryptographic instruction and execution logic. The cryptographic instruction is received by a computing device as part of an instruction flow executing on the computing device, wherein the cryptographic instruction prescribes ~~one of the cryptographic operations~~an encryption operation to be executed on a plurality of input text blocks that are in memory to generate a corresponding plurality of ciphertext blocks, and to store the corresponding plurality of ciphertext blocks in said memory, and where the cryptographic instruction also prescribes one of a plurality of block cipher modes to be employed in accomplishing the ~~one of the cryptographic operations~~encryption operation. The execution logic is operatively coupled to the cryptographic instruction and executes the ~~one of the cryptographic operations~~encryption operation. The execution logic includes a cryptography unit that executes a plurality of cryptographic rounds on each of the plurality of input text blocks to generate a corresponding ~~each of a plurality of output text blocks~~one of said plurality of ciphertext blocks, where the plurality of cryptographic rounds are prescribed by a control word that is provided to the cryptography unit, and where the plurality of input text blocks are retrieved from said memory ~~memory~~, and where the plurality of ~~output text blocks~~corresponding ciphertext blocks are stored to the memory. The ~~one of the cryptographic operations~~encryption operation includes indicating whether the ~~one of the cryptographic operations~~encryption operation has been interrupted by an interrupting event.

[0022] One aspect of the present invention contemplates a apparatus for performing cryptographic operations. The apparatus includes a cryptography unit within a device, block pointer logic, and a bit within a register. The cryptography unit executes ~~one of the cryptographic operations~~decryption operation responsive to receipt of a cryptographic instruction within an instruction flow that prescribes the ~~one of the cryptographic operations~~decryption operation, ~~where the cryptographic instruction also specifies one of a plurality of block cipher modes to be employed when performing said one of the cryptographic operations, and~~ where the cryptography unit is configured execute a plurality of cryptographic rounds on each of a plurality of input data blocks to generate a corresponding each of a plurality of ~~output data~~plaintext blocks, and where the plurality of input data blocks are retrieved from memory, and where the plurality of plaintext~~output data~~ blocks are stored to the memory. The block pointer logic is operatively coupled to the cryptography unit. The block pointer logic is configured to direct the device to modify pointers to the plurality of input and ~~output data~~plaintext blocks in memory to point to next input and ~~output data~~plaintext blocks at the completion of the ~~one of the cryptographic operations~~decryption operation on a current input data block. The bit within the register is operatively coupled to the cryptography unit. The bit indicates that execution of the ~~one of the cryptographic operations~~decryption operation has been interrupted by an interrupting event.

[0023] Another aspect of the present invention comprehends a method for performing cryptographic operations in a device. The method includes fetching a cryptographic instruction from memory, wherein the cryptographic instruction prescribes one of the cryptographic operations along with one of a plurality of block cipher modes to be employed when performing the ~~one of~~one of the cryptographic operations; retrieving a plurality of input data blocks from memory; employing the one of a plurality of block cipher modes and executing the one of the cryptographic operations on the plurality of input data blocks to generate a corresponding plurality of output data blocks, where the executing is performed responsive to the fetching; storing the corresponding plurality of output text blocks to the memory; and indicating whether an interrupting event has occurred during said executing.